STATE OF ALABAMA

Information Technology Standard

Standard 670-08S1: Secure System Maintenance

1. INTRODUCTION:

System (hardware, firmware, software) maintenance, diagnostic, and repair activities may be conducted in-house or by individuals communicating through an external, non-organization-controlled network (e.g., the Internet) further exposing systems to attack. The intent of these requirements is to address the security-related issues arising from information system maintenance, diagnostic, and repair actions.

2. OBJECTIVE:

Ensure all maintenance, diagnostic, and repair activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location, are managed and monitored to preserve the confidentiality, integrity, and availability of State information system resources.

3. SCOPE:

These requirements apply to all personnel (State employees, contractors, vendors, and business partners) responsible for the authorization, administration, and maintenance of State of Alabama information system resources.

Hardware and/or software components that may support information system maintenance, but are a part of the system (e.g., the software implementing “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of an Ethernet switch) are not addressed in these requirements.

4. REQUIREMENTS:

The following requirements, based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-53: *Recommended Security Controls for Federal Information Systems and Organizations*, address the information security aspects of State/agency information system maintenance programs.

4.1 CONTROLLED MAINTENANCE

Policy: The IT Manager shall schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.

IT Manager approval is required before removing information system or system components from organizational facilities for off-site maintenance or repairs.

Maintain control of State data by (i) verifying that there is no organizational information contained on the equipment; (ii) sanitizing the equipment; or (iii) retaining the equipment within the facility. State IT Standard 680-01S4 provides guidance on media sanitization.

Obtain Data Owner approval before authorizing removal of equipment from a State facility when that equipment contains State data.

Following maintenance or repair actions check all potentially impacted security controls to verify that the controls are still functioning properly.

Maintain information system maintenance records for the life of the system that include:

- Date and time of maintenance
- Name(s) of the individual(s) performing the maintenance
- Name of escort (if necessary)
- Description of maintenance performed
- List of equipment removed or replaced (including identification numbers if applicable)

4.2 MAINTENANCE TOOLS

Policy: The IT Manager shall approve and monitor the use of information system maintenance tools.

The IT Manager shall maintain versioning and licensing information for all maintenance tools. Maintenance tools include diagnostic and test equipment (e.g., network or application scanners, hardware or software packet sniffers, etc.) used to conduct maintenance on information systems.

Inspect all maintenance tools brought into a facility by maintenance personnel for obvious improper modifications. Inspect all maintenance tools leaving a facility to verify that there is no organizational information contained on the equipment

Check all diagnostic and test program media for malicious code before use.

Approved maintenance tools shall be documented in system operating procedures.

Requests (with justification) for approval of additional maintenance tools shall be submitted to the IT Manager via email.

4.3 REMOTE MAINTENANCE

Policy: The IT Manager shall authorize and monitor remotely executed maintenance and diagnostic activities.

Log all remote maintenance, diagnostic, and service activities. Maintenance logs should be reviewed daily, but shall be reviewed at least weekly.

Describe the use of remote diagnostic tools, and address the installation and use of remote diagnostic links, in system security plans.

Maintenance personnel shall notify the System Administrator or IT Manager when remote maintenance is planned (i.e., date/time).

Apply security controls (e.g., authorization, authentication, encryption, etc.) to the remote maintenance access connection in accordance with applicable State standards.

Whenever possible, utilize two-factor authentication on remote maintenance ports.

Ensure that remote maintenance access is normally blocked unless unattended access is required. Whenever possible, require some involvement of local personnel in opening remote maintenance ports.

Keep maintenance terminals in locked, limited-access areas.

Whenever possible, turn off maintenance features when not needed.

When remote maintenance is completed terminate all sessions and remote connections. If password-based authentication was used during remote maintenance, change the passwords following each remote maintenance service.

4.4 MAINTENANCE PERSONNEL

Policy: The IT Manager shall maintain a list of authorized maintenance personnel including third-party maintenance providers.

Allow only authorized personnel to perform maintenance on State information systems.

When maintenance personnel do not have the needed access authorizations, organizational personnel with appropriate access authorizations and sufficient technical competence shall supervise maintenance personnel during the performance of information system maintenance activities.

Third-party maintenance providers under contract to perform maintenance/support services on State information system shall provide a list of field service engineers assigned to support State maintenance contract with the following information for each service representative:

- Name
- Company represented
- Title
- Contact Info (phone number; email)
- Photo for identification purposes
- List of systems individual is authorized to perform maintenance on

4.5 TIMELY MAINTENANCE

Specify the security-critical information system components that, when not operational, result in increased risk to the organization, individuals, or the State because the security functionality intended by that component is not being provided. Security-critical components may include, for example, firewalls, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems.

Conduct a risk assessment and analysis/determination of need for the continuity of operations of security-critical information system components to determine the maximum tolerable downtime duration.

Ensure maintenance support and spare parts for the identified list of security-critical information system components is obtained within the defined time period.

The IT Manager shall document these maintenance requirements in operational procedures.

5. ADDITIONAL INFORMATION:

5.1 POLICY

Information Technology Policy 670-08: System Maintenance
http://isd.alabama.gov/policy/Policy_670-08_System_Maintenance.pdf

5.2 RELATED DOCUMENTS

Information Technology Standard 680-01S4: Media Sanitization
http://isd.alabama.gov/policy/Standard_680-01S4_Media_Sanitization.pdf

Signed by Art Bess, Assistant Director

6. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	7/9/2009	Replaced State IT Standard 640-02S4